Forensic Report – Preliminary

Joshua Marpet
Managing Principal

2/28/2014

GUARDED RISK

Background:

This report is written by Joshua Marpet, Managing Principal of Guarded Risk. Joshua Marpet is an Adjunct Professor teaching Digital Forensics, Information Security, Ethics, and Ethical Hacking at Wilmington University, in the College of Technology, Computer Network Security program. Joshua is an Accessdata Certified Examiner (ACE) in the field of digital forensics. Joshua Marpet is a former Senior Information Security Analyst at the Federal Reserve Bank of Philadelphia. He is a co-organizer of the Security BSides Delaware series of Information Security Conferences, and is the Vice President of the Cloud Security Alliance, Delaware Valley Chapter (CSA-DV). His background includes being a police officer with the St. Tammany Parish Sheriff's Office before, during, and after Hurricane Katrina. Joshua Marpet's experience also includes work on video and audio surveillance systems around the world, including the Lower Manhattan Surveillance Initiative, Algerian military base fence alarm systems, and Newark Airport's tarmac surveillance, along with multiple prisons and casinos.

Request:

An MP3 file was provided, and a request was placed to determine, as conclusively as possible, if any "tampering" had been performed on the audio.

Issues:

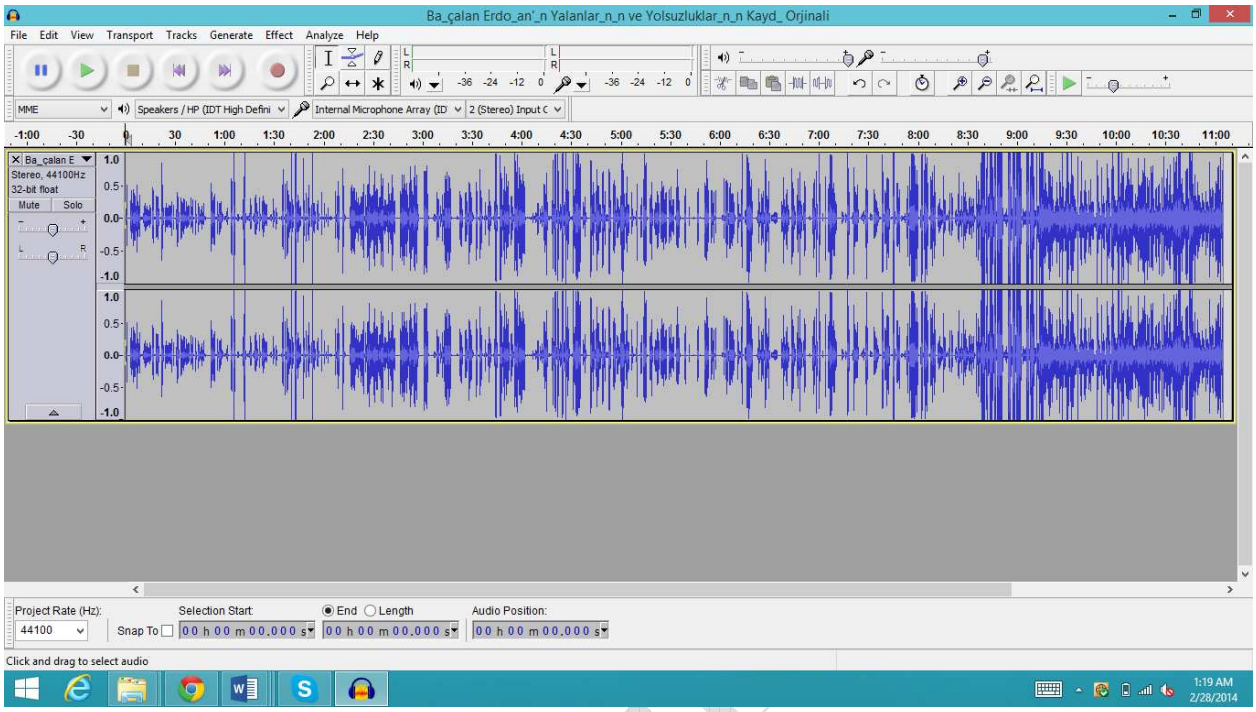
Not being a native Turkish speaker, it's difficult to determine intonation changes, nuances, tonal changes, and whether a word or phrase has ended abruptly, or out of sync. That being said, it was determined to perform a technical analysis of the audio, and confirm any anomalies or questions with the help of native Turkish speakers as part of the analysis.

Tools:

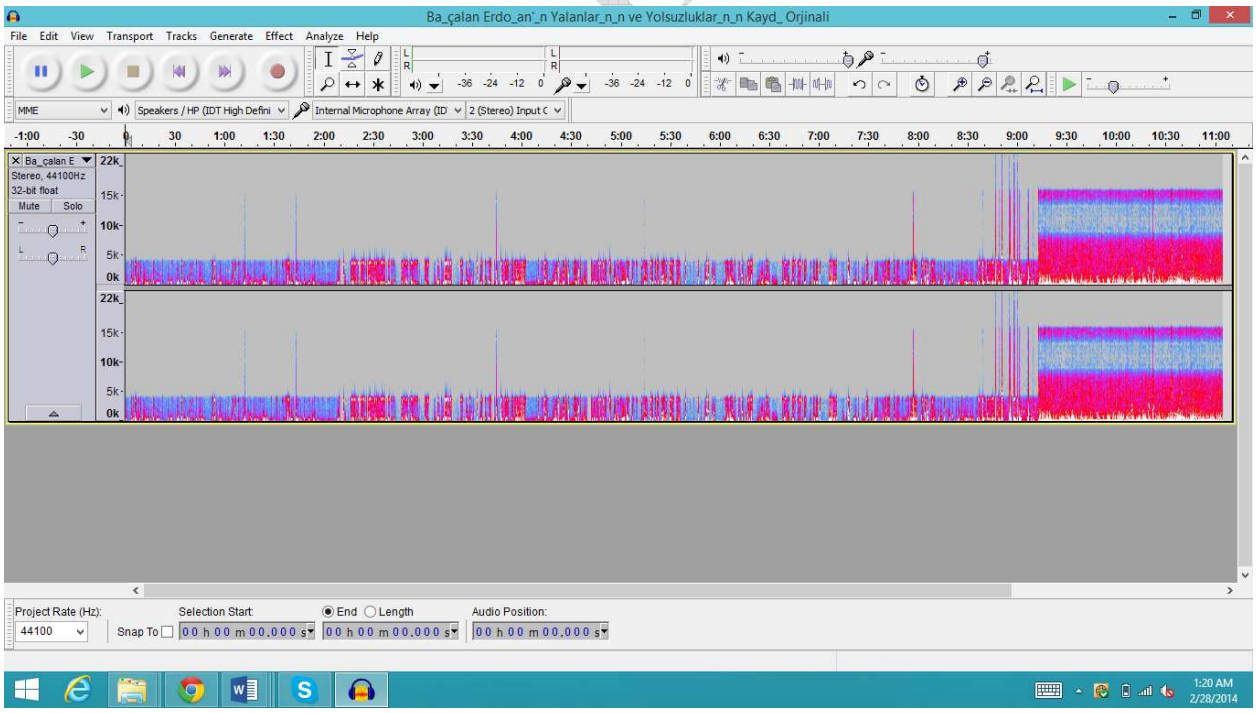
An HP laptop, running Microsoft Windows 8.1, and fully patched, was utilized to perform the analysis. The software used was Audacity from http://audacity.sourceforge.net/. It is a highly capable audio creation and editing software, used in multiple ways, from podcast creator and editor, to music editing and mixing. As an open source project, its code is examined and tested by hundreds of thousands of people.

Analysis:

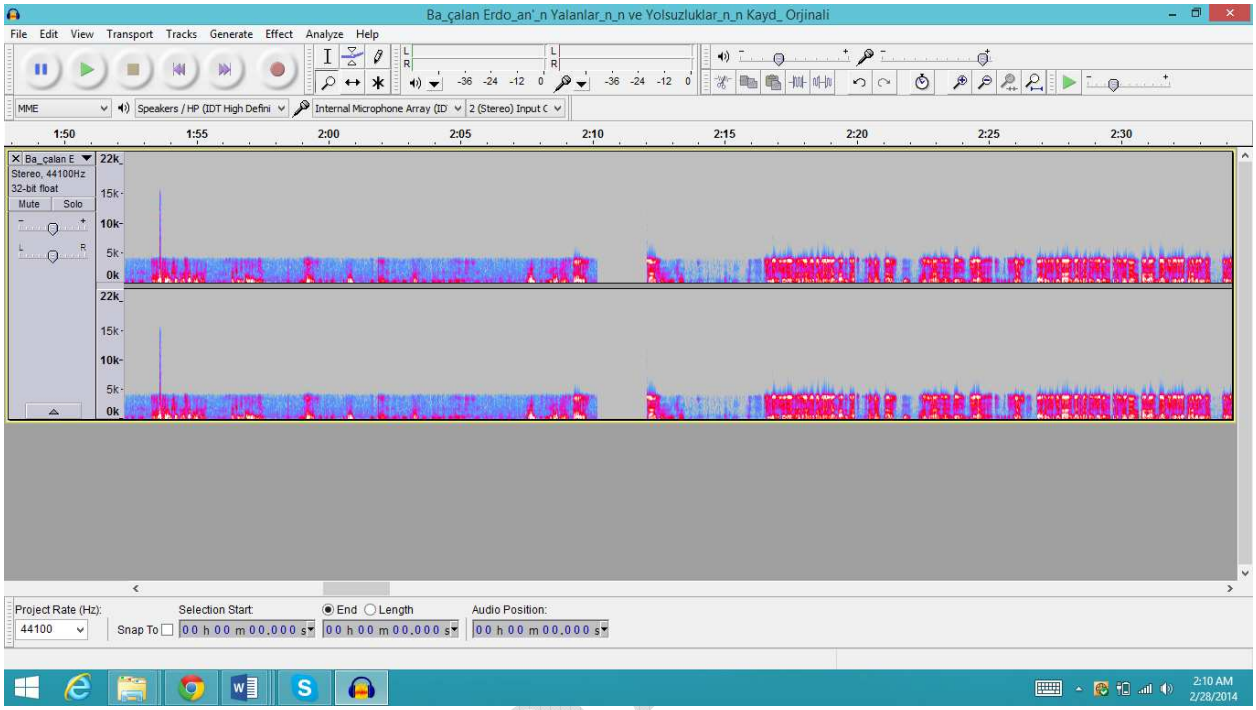
An MP3 file, named “Ba_çalan Erdo_an'_n Yalanlar_n_n ve Yolsuzluklar_n_n Kayd_ Orjinali.mp3”, was provided for analysis. Opening it in Audacity shows the waveform view, roughly correlating to volume.



Switching to Spectrogram view shows a frequency plot.



In this view, which was the primary view used for analysis, three sets of anomalies were discovered. It can be seen that while most of the conversation is on the same level, the "noise floor", there are several frequency "spikes" scattered throughout the audio, and the last few minutes, from approximately 9:15 on, are on a totally different noise floor. The last set of anomalies can only be easily seen when zoomed in.


Ba_çalan Erdo_an'_n Yalanlar_n_n ve Yolsuzluklar_n_n Kayd_ Orjinali
File Edit View Transport Tracks Generate Effect Analyze Help
1:50 1:55 2:00 2:05 2:10 2:15 2:20 2:25 2:30
Project Rate (Hz):
Selection Start:
Audio Position:
2:10 AM
2/28/2014

Between 2:10 and approximately 2:12, seen above, there is a gap with absolutely no sound at all. If this mp3 is played, even when there are no voices, there is environmental and electronic noise, from air conditioning, heating systems, line noise on the phone, etc. But from 2:10 to 2:12, there's nothing at all.

One of the frequency "spikes" can be noted just before 1:54 in the figure above, as well.

Assuming malicious intent for all three sets of anomalies, the gaps could be indicative of cutting and pasting segments of sound, and the spikes attempting to change the tone, intonation, nuance, or meaning of a word or phrase. The raised noise floor and different voices for the last few minutes of audio could be indicative of a different type of bug, that of a room bug, rather than a phone bug. Alternatively, it could simply have been the same phone turned on it's speakerphone.

Consultation with a Turkish speaker:

A Turkish speaker was consulted about the anomalies.

The first anomalous piece discussed was the gaps, such as the one at 2:10. As it turns out, the gaps are simply where the multiple recordings were placed together in one mp3 file. Not malicious at all.

The raised noise floor of the last few minutes was identified as a joke, or added bit of dialogue with people not involved in the phone calls. It was speculated that they could be the people who leaked the phone calls?

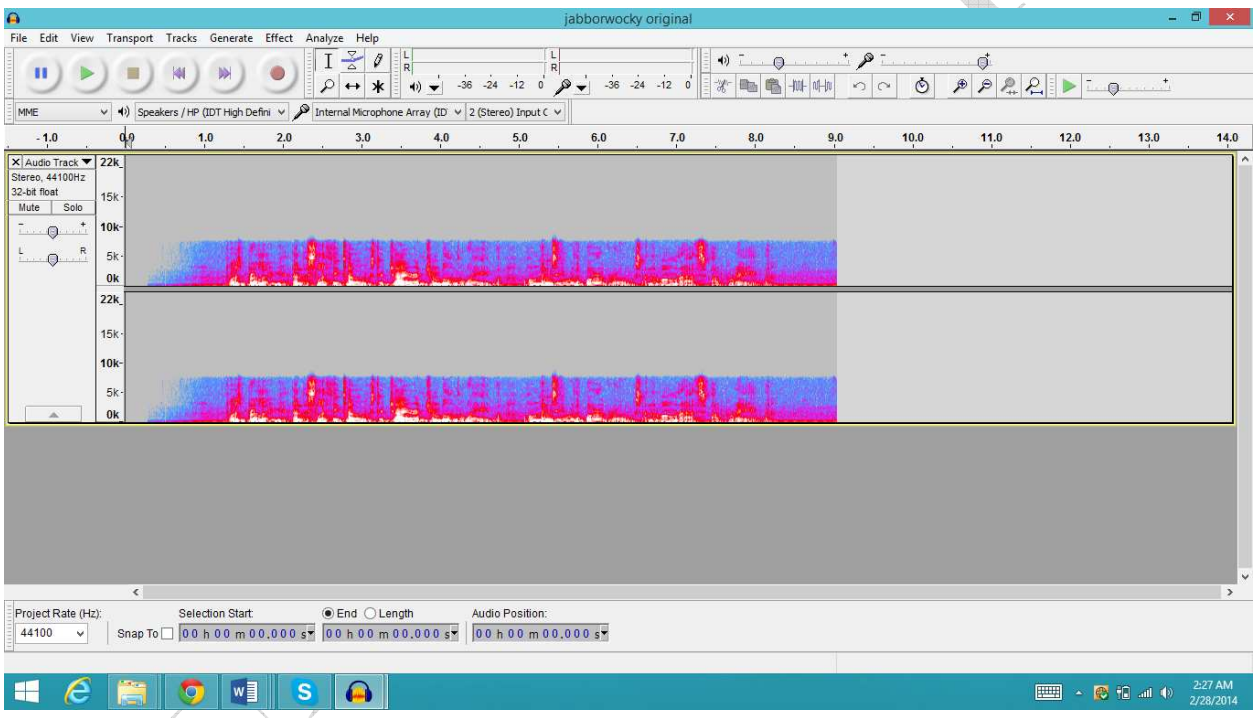
GUARD

The only anomaly that is unsolved is the “spikes”. The two possibilities discussed at that point were cutting and pasting of audio, or an attempt to change the tone, intonation, nuance, or meaning of a word or phrase. The Turkish speaker indicated that the tone, intonation, nuance, and meaning appeared to be natural, without artificial change. Also, the spikes occurred, almost without fail, after sound had already started, meaning that if they were an indication of cutting and pasting, the sound should have changed abruptly at those moments, in the middle of a word, for example.

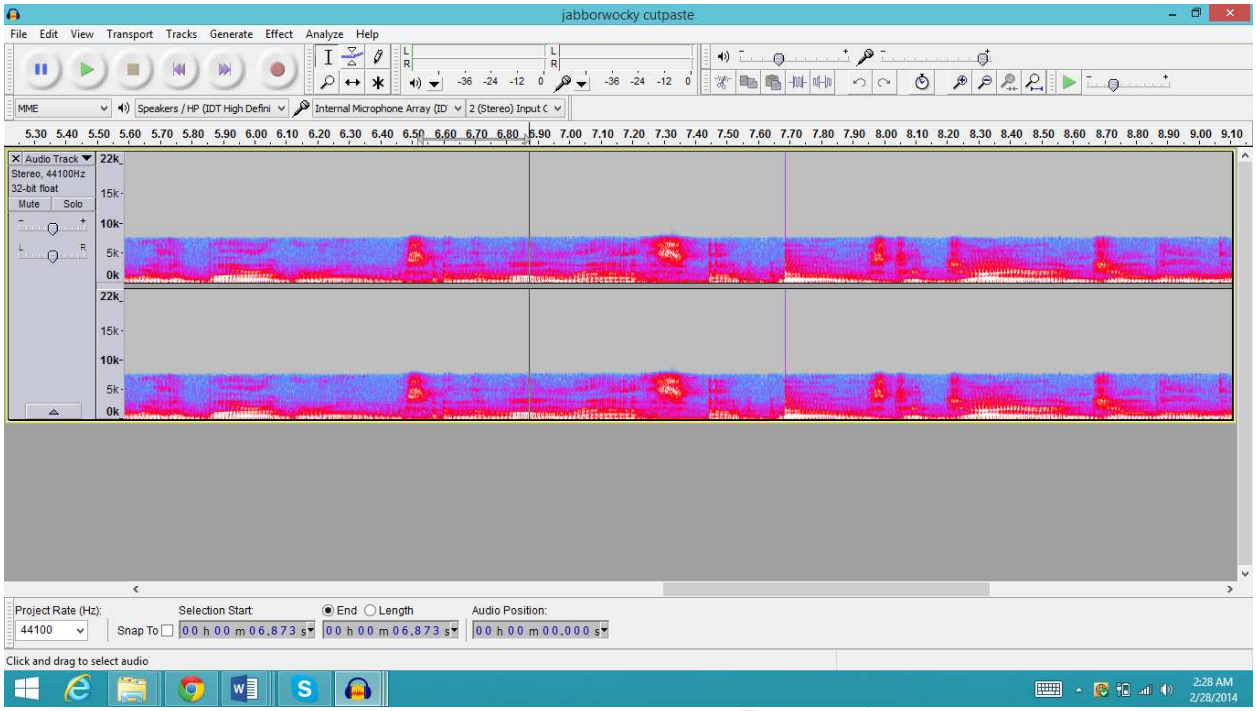
A supposition, or guess, is that the spikes are some sort of bookmark, or index. Many of them seem to be markings near or on names. This has not been explored due to time constraints.

Conclusions:

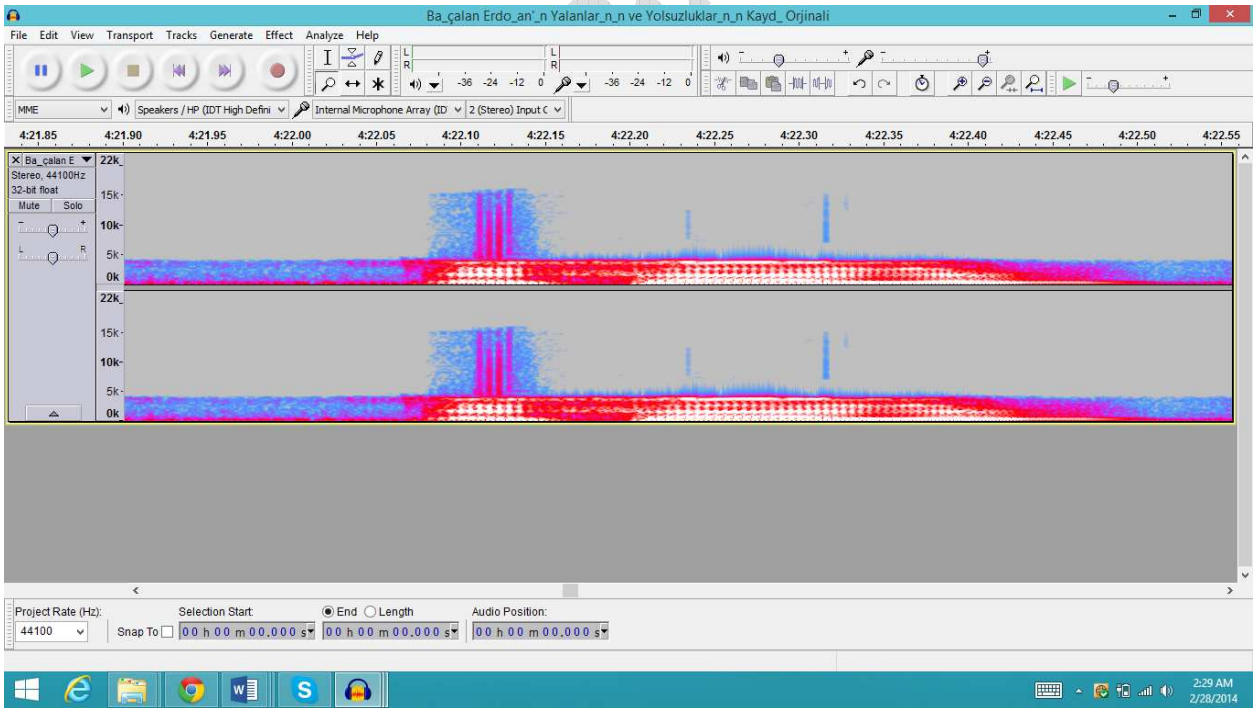
To check these conclusions and suppositions, a short audio track was recorded, using the HP laptop, and Audacity, listed above in the Tools section. Joshua Marpet recited the first verse of Lewis Carroll’s “Jabberwocky” poem. (Jabberwocky original).

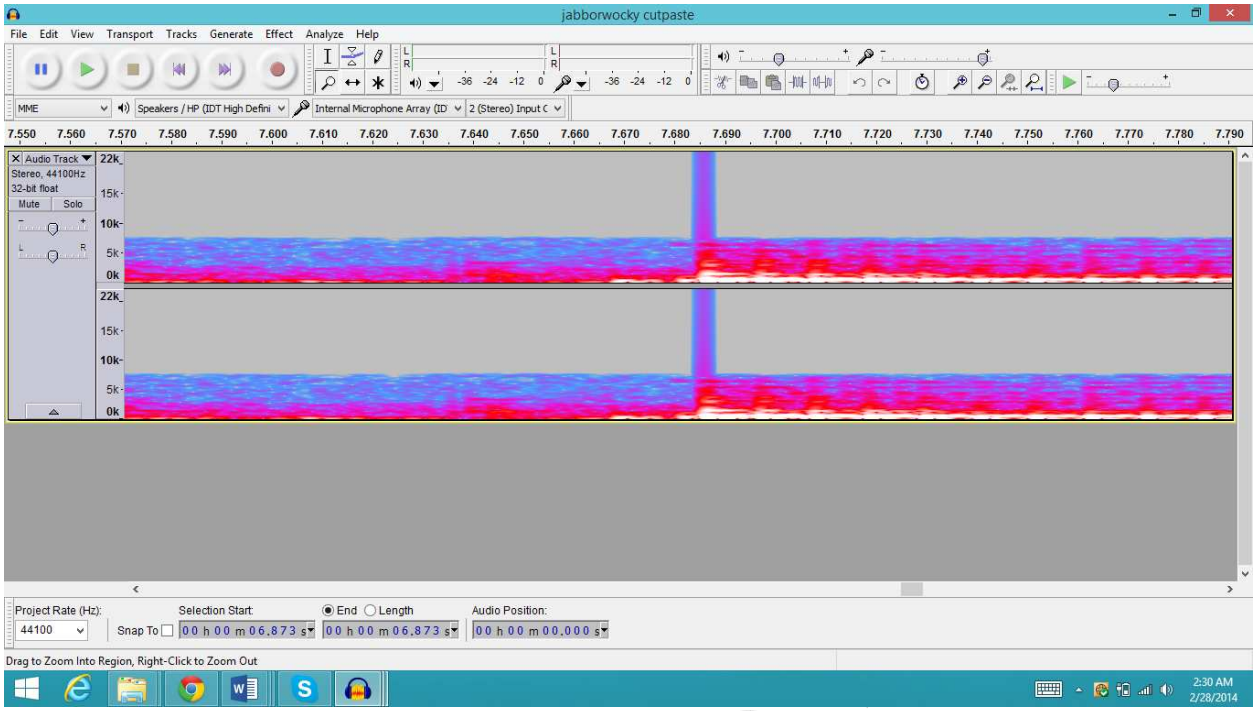


He then cut and pasted a short section of it, to a later area of the poem.



Notice the two spikes, which in some ways are similar to the frequency spikes in the first examined recording. However, they are different in some important ways. Upon zooming in, these ways become obvious.





Notice how clean the line is in the Jabberwocky recording, and how it reaches to the top of the channel/spectrogram. Notice how in the Turkish call recording, it is actually multiple lines, not clean at all, with much "static" around it, and how it does not reach to the top of the channel/spectrogram.

This indicates that the frequency spikes are indeed artifacts, but most likely from some line noise, clicking, or indeed, still possibly a bookmarking or annotation system. It was checked with the Turkish speaker, and most of the spikes in the Turkish call recording were in the middle of names and words. Any cut and paste would have mangled those names and words.

Final Conclusions:

The Turkish call audio recording, minus the "joke" last few minutes, appear to be recordings of multiple calls (the gaps), without any cutting, pasting, collaging, or any tampering whatsoever. While it cannot be proven to be truly tamper free without access to the original source material, and an unbroken chain of custody, at this point, we are unable to prove that it was tampered with in any way.

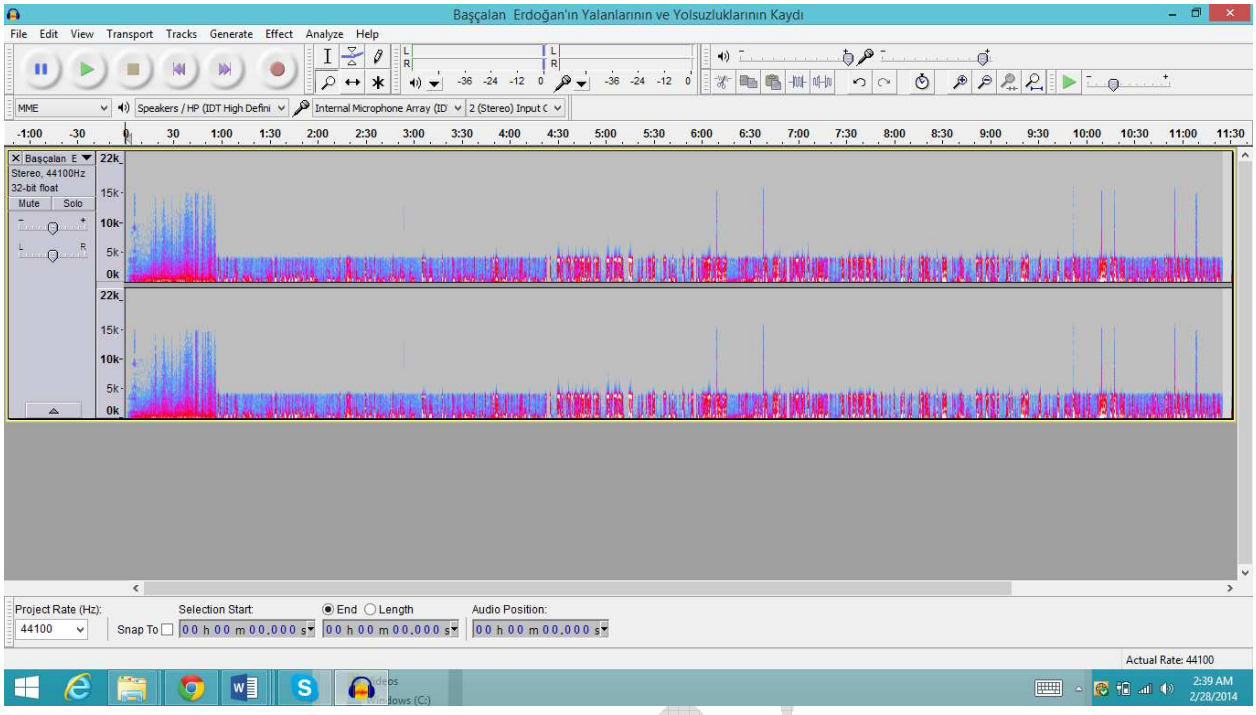
Addendum 1: different source material for original set of recordings

https://www.youtube.com/watch?v=Cvf4aeRLu0E - Başçalan Erdoğan'ın Yalanlarının ve Yolsuzluklarının Kaydı

Using the above youtube link, and an online youtube to MP3 converter, an MP3 of this youtube video was obtained. While similar in many ways to the source material supplied by Roy Gutman, the McClatchy reporter, there are some differences. There is music at the start of the audio, skewing the time codes. The last few minutes do not have the "joke" section.

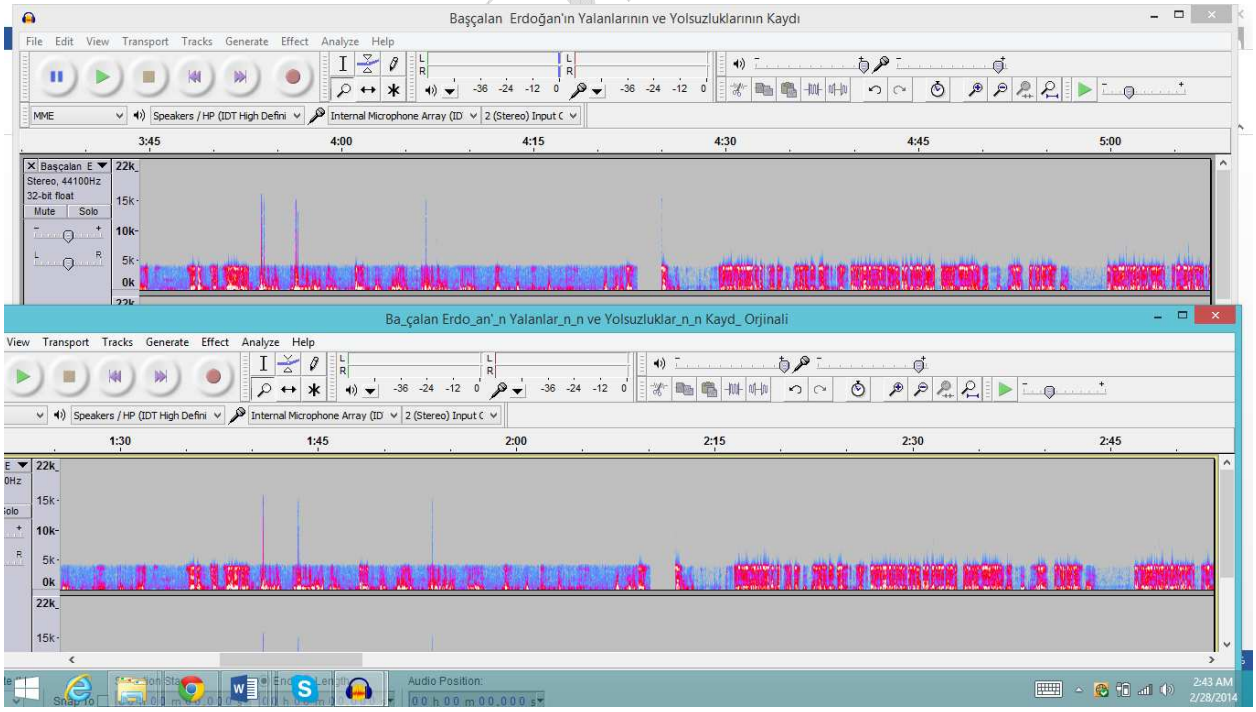
GUARDED

However, the gaps, and the spikes remain.



In order to compare, the gap that is found at 2:10 in the audio supplied by Roy Gutman, was located in this audio at approximately 4:23.

The gaps, and the several spikes preceding it, line up fairly precisely.


Başçalan Erdoğan'ın Yalanlarının ve Yolsuzluklarının Kaydı
Ba_çalan Erdo_an'_n Yalanlar_n_n ve Yolsuzluklar_n_n Kayd_ Orjinali

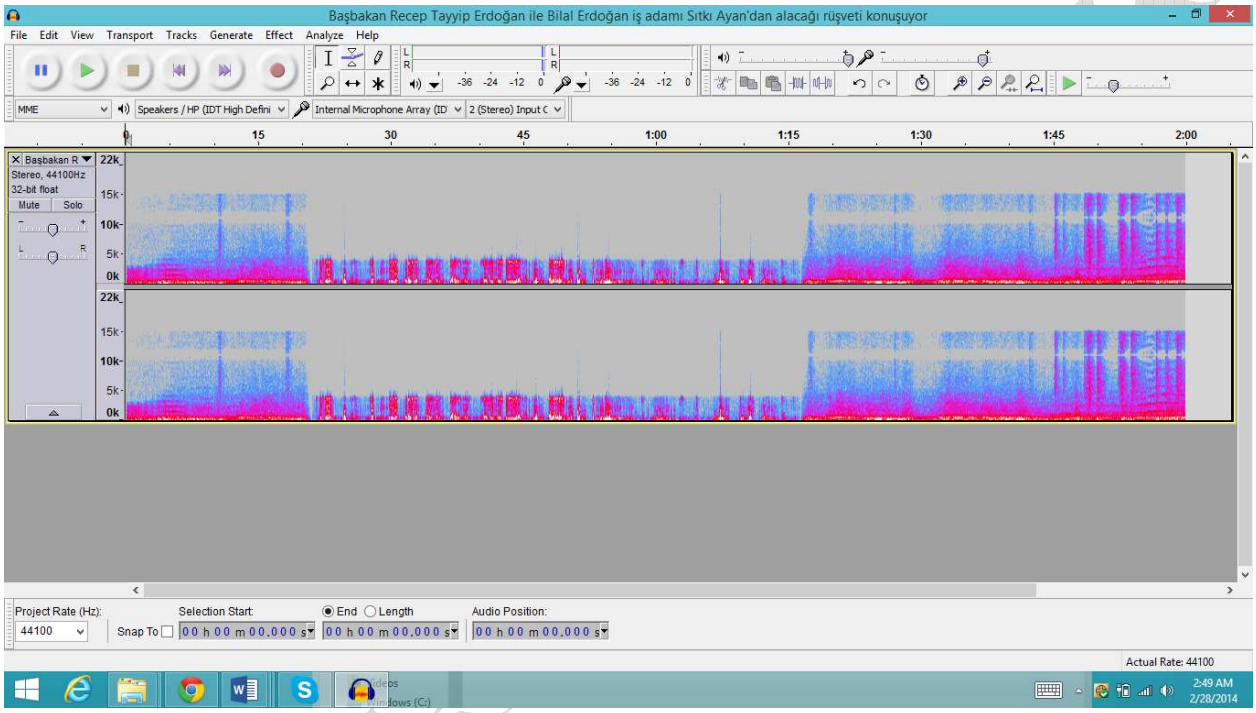
The recordings, minus the music at the start of the one, and the “joke” at the end of the other, matched.

The same conclusions can be drawn. At this time, they cannot be proven false.

Addendum 2: Second Set of recordings

Using this Youtube link, a second set of recordings was obtained. Using the same online Youtube to MP3 converter, an audio file was obtained and examined using the same tools as before, namely, the HP laptop running Windows 8.1, and the Audacity software.

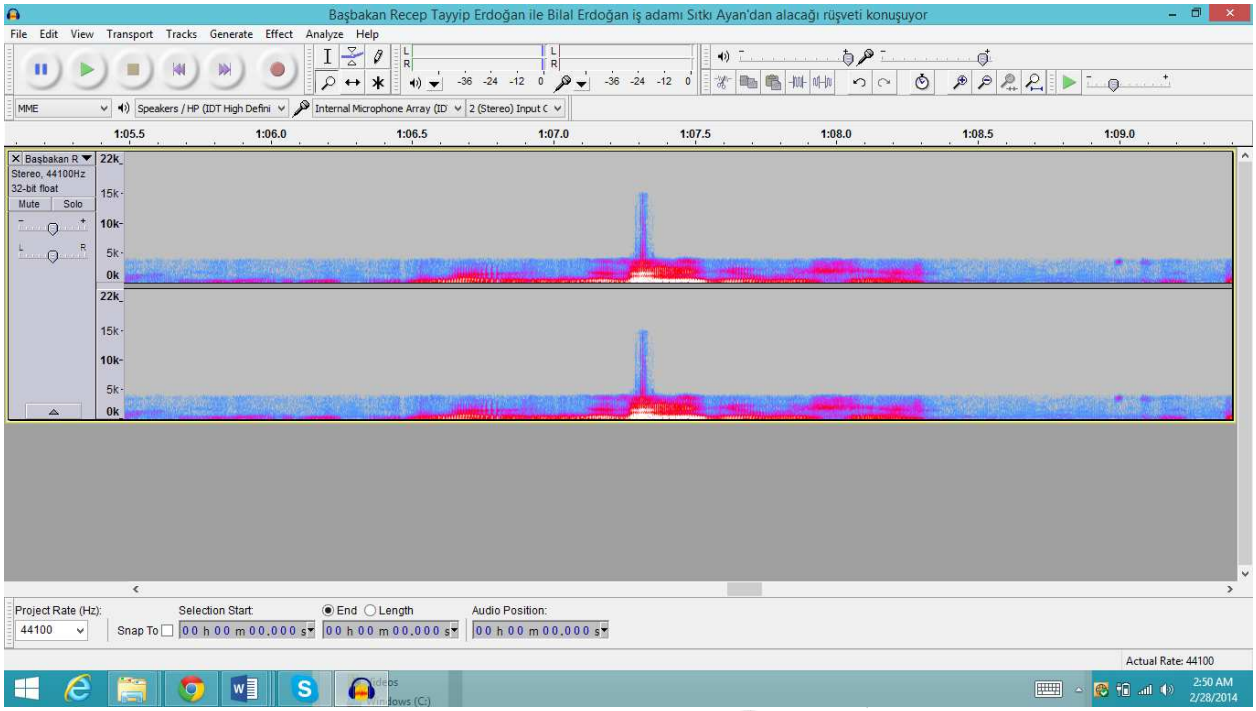
http://www.youtube.com/watch?v=Ya1iQvpxe60 – 2nd set - Başbakan Recep Tayyip Erdoğan ile Bilal Erdoğan iş adamı Sıtkı Ay


Başbakan Recep Tayyip Erdoğan ile Bilal Erdoğan iş adamı Sıtkı Ayan'dan alacağı rüşveti konuşuyor
File Edit View Transport Tracks Generate Effect Analyze Help
Project Rate (Hz):
Selection Start:
End
Length
Audio Position:
Actual Rate: 44100

Notice the raised Noise Floors at the beginning and end of the recording. This is music, and in no way relates to the phone call itself.

The largest spike in the call was magnified to determine its origin.

GUARD



It is similar in composition, and in "look", to the spikes from the first set of recordings. As it occurs, again, after vocalization of the word has started, it is extremely unlikely that it is a cut and paste, or montage of sounds.

Again, at this point, with this recording, and no access to original source material with an unblemished chain of custody, this cannot be proven to be false, to the limits of our engineering certainty.

Addendum 3:

Interest has been expressed in Cryptophones, and how the recordings might have been obtained in the first place. Please note, this is all supposition and informed guess.

Cryptophones, classically, have an encrypted tunnel with a server. The server and phone have a pair of keys. What is encrypted with one key can be decrypted with the other, and vice versa. But each phone and server key pair is unique, for that phone only. What that means, practically, is that Phone 1 connects to the server. Phone 2 connects to the server. Then the person holding Phone 1 can talk through the phone, down the encrypted tunnel, to the server, across the server, to the encrypted tunnel to Phone 2, where the person holding Phone 2 will hear it.

Since the server has the keys to decrypt and encrypt all traffic to and from Phone 1 and Phone 2, whoever controls the server can listen to both sides of the conversation.

As far as is known today, only one commercial company has the capability to avoid this. Silent Circle, which was formed from the same people who created PGP (Pretty Good Privacy) encrypted email, uses keys from phone to phone, not phone to server to phone. This is known as a "Zero-Knowledge" system, where even the people who run the system cannot decrypt or have any knowledge of the use or data on the system.

GUARDED

Recordings:

The recordings have one thing in common that is interesting in this context. The younger man on the calls is loud, clear, almost overpowering the microphone on the phone. The older gentleman's voice is quieter, and a bit fuzzier, or "pixilated".

While the reasons for this are not known, some can be supposed.

1. It is possible that one person was on a cryptophone, which compresses, digitizes, and encrypts the audio. In that case, the fuzziness and low volume could be explained by that.
2. On the other hand, if the younger gentleman's phone was bugged, then the loudness of his voice could be explained by the physical nearness of it. He would be speaking directly into the bug, while the older gentleman would be received through the phone circuitry, adding fuzziness and lowering the volume. Realize that the "bug" could be a software program, a piece of malware, rather than a physical bug.
3. One last case, if both parties were on cryptophones, and the intercept was from the central server, perhaps one of the parties was simply almost out of data range, resulting in lowered bandwidth.

All of these cases in this Recording segment, are thought experiments. None of them are based directly on reality, as no reliable information as to the real situations has been received. They are listed here as possibilities.

This report is the truth, with the information I have, and to the limits of the knowledge and experience I possess.

Joshua Marpet

Managing Principal

Guarded Risk

2/28/2014

GUARDED RISK